E. MARTIN ESTRADA
United States Attorney
MACK E. JENKINS
Assistant United States Attorney
Chief, Criminal Division
MARK A. WILLIAMS (Cal. Bar No. 239351)
Chief, Environmental and Community Safety Crimes Section
MATTHEW W. O'BRIEN (Cal. Bar No. 261568)
JUAN M. RODRIGUEZ (Cal. Bar No. 313284)
Assistant United States Attorneys
Environmental and Community Safety Crimes Section
BRIAN R. FAERSTEIN (Cal. Bar No. 274850)
Assistant United States Attorney
Public Corruption and Civil Rights Section
1300/1500 United States Courthouse
312 North Spring Street
Los Angeles, California 90012
Telephone: (213) 894-3359/8644/3819/0304
E-mail: Mark.A.Williams@usdoj.gov
Matthew.O'Brien@usdoj.gov
Brian.Faerstein@usdoj.gov
Juan.Rodriguez@usdoj.gov

Attorneys for Plaintiff
UNITED STATES OF AMERICA

UNITED STATES DISTRICT COURT

FOR THE CENTRAL DISTRICT OF CALIFORNIA

UNITED STATES OF AMERICA, Plaintiff, v. JERRY NEHL BOYLAN, Defendant.	No. CR 22-482-GW GOVERNMENT'S OPPOSITION TO DEFENDANT'S MOTION TO COMPEL GOVERNMENT TO PERMIT DEFENSE EXAMINATION OF DIGITAL DEVICES OR TO EXCLUDE DATA FROM THE DEVICES AT TRIAL IN THE ALTERNATIVE (DKT. NO. 28); EXHIBITS 1-5 Hearing Date: April 24, 2023 Hearing Time: 8:00 a.m.

Plaintiff United States of America, by and through its counsel of record, the United States Attorney for the Central District of California and Assistant United States Attorneys Mark A. Williams, Matthew W. O'Brien, Brian R. Faerstein, and Juan M. Rodriguez, hereby files its Opposition to Defendant JERRY NEHL BOYLAN's Motion to

Compel Government to Permit Defense Examination of Digital Devices or to Exclude Data from the Devices at Trial in the Alternative (Dkt. No. 28).

This Opposition is based upon the attached memorandum of points and authorities and accompanying exhibits, the files and records in this case, and such further evidence and argument as the Court may permit.

Dated: March 30, 2023

Respectfully submitted,

E. MARTIN ESTRADA
United States Attorney

MACK E. JENKINS
Assistant United States Attorney
Chief, Criminal Division

/s/
MARK A. WILLIAMS
MATTHEW W. O'BRIEN
BRIAN R. FAERSTEIN
JUAN M. RODRIGUEZ
Assistant United States Attorneys

Attorneys for Plaintiff
UNITED STATES OF AMERICA

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page(s)

Cases

Statutes

//

//

Rules

Other Authorities

MEMORANDUM OF POINTS AND AUTHORITIES

I. INTRODUCTION

Undeterred by the constraints imposed by the Constitution and Rule 16, defendant seeks private information on iPhones that belonged to innocent victims who died in the fire aboard the *Conception*. Without citing a single criminal case in which a court compelled the government to provide a full, mirrored copy of a victim's phone to a defendant, the defense asks the Court to order the government to provide defendant with everything contained on the victims' devices. In the defense's view, all of the victims' contacts, family photos, videos with friends, personal notes, and text messages are defendant's to review. Not so.

Defendant's motion to compel is rooted on a flawed premise. The defense contends the government purportedly "faces a choice": either it hands over complete copies of victims' digital devices containing voluminous private information that has already been lawfully reviewed for responsiveness, or it forfeits its ability to present at trial the limited responsive information seized from those devices. (Dkt. No. 28 ("Mot.") at 2.) But no such "choice" exists under the law or the facts of this case.

First, defendant glosses over the fact that the government no longer has access to these digital devices after its initial review pursuant to search warrants and limited consents. The unseized data on the devices are consequently not within the possession, custody, or control of the government. Second, the devices fall within the core privacy interests protected by the Fourth Amendment and cannot be turned over to the defense. Third, the defense fails to make any credible showing of materiality, as it must under Federal Rule of

Criminal Procedure 16, with respect to the voluminous data on the devices that was found to be non-responsive pursuant to the government's lawful review. Taken to its logical conclusion, the essence of the defense's materiality theory -- namely, that defendant should be able to check the government's work -- would eviscerate Federal Rule of Criminal Procedure 41 and the foundational principles of the Fourth Amendment.

The defense's attempt to frame the issue, falsely, as a "choice" on the government's part, without any legal authority on point, appears to be a backdoor attempt to suppress critical evidence that the government lawfully obtained. Most notably, one of the victim's phones contained a video, taken during the deadly fire, showing that the passengers were alive but trapped in the ship's bunkroom three minutes after defendant abandoned ship and ordered his crew to do the same.

Last year, the Honorable John F. Walter denied a nearly identical (but less factually attenuated) motion filed by the Federal Public Defender's Office. In that case, the defendants sought to compel the production of complete copies of digital devices that belonged to cooperators (not victims, as here). Judge Walter found that the government no longer possessed the previously searched devices and the defendants failed to demonstrate the requisite materiality of the unseized data. (See United States v. Jose Luis Huizar et al., Case No. CR 20-326(A)-JFW (Dkt. Nos. 436, 597 at 33-38).) Undeterred by Judge Walter's ruling, the defense makes the same pitch to this Court.

Defendant will be on trial, not the victims of his crime. He has no legal basis to examine the private information contained on their iPhones. The motion should be denied.

II. RELEVANT FACTUAL BACKGROUND

On September 2, 2019, a fire aboard the *Conception* killed all thirty-three passengers and the youngest crewmember who had been sleeping below deck when the fire started. It was a preventable tragedy. Defendant was the captain in charge of all operations aboard the *Conception*, but on the night of the fire he went to sleep without ordering any night watch or roving patrol. When a crewmember finally woke up and discovered the fire, defendant failed to order any firefighting or lifesaving operations (he had never trained the crew on how to respond to a fire). Defendant was the first person to abandon ship, despite the fact that everyone below deck was still alive.

After the fire, first responders conducted extensive search and rescue activities, and local, state, and federal agencies began parallel investigations and inquiries related to the incident. As part of the federal criminal investigation, on September 7, 2019, search warrants were issued by the Hon. Louise A. LaMothe for evidence related to the *Conception*, the *Conception's* sister ships, and Truth Aquatics Inc. (the *Conception's* owner). (See Dkt. No. 28-1, Exh. C.) Agents executed the search warrants and obtained extensive documentary and physical evidence, including dozens of digital devices. Defendant's motion to compel appears to be limited to the victims' digital devices seized from the *Conception* wreckage that were searched and found to contain responsive information,

including evidence the government intends to offer at trial (the "Subject Devices").[1]

Specifically, the victims' digital devices recovered from the ocean were sent to FBI's laboratory in Quantico, Virginia, for review and analysis. Given the significant fire and water damage, the technical review process required substantial time and expertise. Due to the damage to the devices, to date FBI specialists have been able to repair only three iPhones and one iPad so that their data were reviewable.[2]

The four reviewable digital devices included an iPad (FBI Device No. 1B177) and an iPhone (FBI Device No. 1B174) that were searched pursuant to the terms and protocols of the first search warrant. The FBI case agent reviewed the data for each digital device through the Cellebrite platform and seized evidence consistent with Attachment B of the search warrant. No relevant evidence was found on the iPad, and the government therefore does not intend to offer evidence from this device at trial. The iPhone was found to contain images and videos of the 2019 dive trip before the fire took place.

---

[1] It is not clear to the government from the motion exactly which digital devices the defense is seeking to compel. The government construes the motion as encompassing only the digital devices from which the government recovered responsive data that it may use at trial (i.e., the Subject Devices). If the defense is seeking a broader set of digital devices, the same arguments that the government sets forth herein would apply.

[2] FBI specialists are attempting to extract data from one badly damaged iPhone (FBI number 1B137) that was recovered from the *Conception* wreckage and was owned by one of the victims whose next-of-kin has provided limited consent. However, it remains unclear whether the iPhone can be rebuilt in order to obtain information from it. Given the incriminating nature of the evidence recovered from the other three digital devices -- including the video showing the victims alive and in need of rescue in the bunkroom after defendant abandoned ship -- it is highly unlikely that material helpful to the defense will be recovered from this phone even if it is found to be reviewable.

The final two reviewable digital devices were iPhones (FBI Device Nos. 1B136 and 1B290). Given the lengthy and technical nature of the digital device review process, the search warrant expired with respect to these iPhones before the review process was complete. Before repairing iPhone 1B136 and reviewing it, the government received consent from the victim's family specifically authorizing FBI agents to seize evidence "related to their investigation." (Dkt. 28-1, Exh. D.) The iPhone was repaired, searched, and found to contain pictures and videos taken during the dive trip. One short video, showing victims alive during the fire, was taken by one of the victims in the bunkroom after defendant abandoned ship.

The government was not able to determine which victim owned iPhone 1B290 and thus could not obtain consent to search the phone. The Hon. John F. Anderson, United States Magistrate Judge for the Eastern District of Virginia, issued a warrant to search and obtain evidence from that iPhone. (See Search Warrant, attached as Exhibit 1 hereto.[3]) The FBI case agent reviewed the data for this iPhone through the Cellebrite platform and seized evidence consistent with Attachment B of the search warrant.

The complete Cellebrite reports for the three reviewable iPhones (i.e., the Subject Devices) were all produced in discovery, including load files of the Cellebrite materials and metadata. (See Discovery letters including indices, attached as Exhibits 2-4 hereto.) The

[3] The search warrant application for iPhone 1B290 attached as exhibits the initial Passenger Vessel Conception Wreckage search warrant and search warrant application, which the defense also independently attached to its motion as Exhibit C. (See Dkt. No. 28-1, Exh. C.) In order to limit the volume of pages attached as exhibits here, the government has removed the redundant exhibits that were attached to the iPhone 1B290 search warrant application in the copy of that search warrant application attached as Exhibit 1 hereto.

discovery includes detailed information for each iPhone and the materials on the phones.

III. LEGAL STANDARD

"There is no general constitutional right to discovery in a criminal case, and Brady did not create one." Weatherford v. Bursey, 429 U.S. 545, 559 (1977). There are three sources of the government's discovery obligations in a criminal case.

First, Rule 16 of the Federal Rules of Criminal Procedure establishes guidelines for pretrial production by the government of seven categories of material, including documents and objects "within the government's possession, custody, or control" that are "material to preparing the defense," that the government intends to use in its case-in-chief at trial, or that was obtained from or belongs to the defendant. Fed. R. Crim. P. 16(a)(1)(E). "A defendant must make a threshold showing of materiality, which requires a presentation of facts which would tend to show that the Government is in possession of information helpful to the defense." United States v. Santiago, 46 F.3d 885, 894 (9th Cir. 1995) (citation omitted).

Second, under Brady v. Maryland, 373 U.S. 83 (1963), and Giglio v. United States, 405 U.S. 150 (1972), the government must turn over evidence in its possession that is favorable to the defense or that may be used by the defense for impeachment purposes. Specifically, Brady "requires disclosure only of evidence that is both favorable to the accused and material either to guilt or to punishment." United States v. Bagley, 473 U.S. 667, 674 (1985) (citation omitted). As the Ninth Circuit has held:

> It is the government, not the defendant or the trial court, that decides *prospectively* what information, if any, is material and must be disclosed under Brady.... And, as the

> Supreme Court has explained, Brady does not permit a defendant to sift through information held by the government to determine materiality. 'A defendant's right to discover exculpatory evidence does not include the unsupervised authority to search through the [government's] files. Although the eye of an advocate may be helpful to a defendant in ferreting out information, **this Court has never held ... that a defendant alone may make the determination as to the materiality of the information.** Settled practice is to the contrary.'

United States v. Lucas, 841 F.3d 796, 807 (9th Cir. 2016) (italicized emphasis in original, bolded emphasis added) (quoting Pennsylvania v. Ritchie, 480 U.S. 39, 59-60 (1987)).

Third, under the Jencks Act, statements by a government witness that relate to the subject matter of the witness's testimony are required to be disclosed to the defense after the witness has testified. 18 U.S.C. § 3500.

Defendant principally relies on Rule 16(a)(1)(E) in seeking to obtain full copies of the digital devices, with only passing references to Brady/Giglio as another purported basis for disclosure. Neither source of discovery entitles defendant to inspect the complete copies of the Subject Devices in this case.[4]

IV. ARGUMENT

A. Defendant Is Not Entitled to Access the Complete Copies of the Subject Devices

Defendant's claim of right to "inspect the complete copies" of the Subject Devices (Mot. at 1) disregards the government's lack of possessory interest in the devices as well as the victim-decedents'

[4] Defendant does not contend, nor could he, that the unseized portions of the Subject Devices are discoverable under the Jencks Act.

significant and Constitutionally protected privacy interests in the unseized data.

1. Information That Is Not Seized Pursuant to a Search Warrant or Consent Is Not in the Possession of the Government

Information is "in the possession of the government" if the prosecutor "has knowledge of and access to the documents sought by the defendant." United States v. Bryan, 868 F.2d 1032. 1036 (9th Cir. 1989); United States v. Cano, 934 F.3d 1002, 1023 (9th Cir. 2019) (same).

As previously explained, the government obtained a court-authorized search warrant in this District for the "Passenger Vessel Conception Wreckage," which included "any digital devices recovered from the P/V CONCEPTION's wreckage and/or debris field." (Dkt. No. 28-1, Exh. C at 11.) The FBI was able to access and search, and seize responsive information from, several of the fire- and/or water-damaged Subject Devices pursuant to the first search warrant (specifically, Device Nos. 1B174 and 1B177). The government obtained three extensions of the allowable review period in order to do so, and the review period expired on December 30, 2020.

Separately, the government obtained a rollback, Court-authorized search warrant from the District Court for the Eastern District of Virginia for one additional device (Device No. 1B290). (See Exh 1.) This device was initially believed to be too damaged to access but later was salvaged through advanced laboratory techniques. (Id.; see also Exh. 4.) The FBI also searched for and seized from this device data responsive to the search warrant, and the 120-day review period expired on December 24, 2022. (Id.)

Pursuant to the terms of the warrants, the government had legal authority during the applicable review periods to access and search the content on those devices for a limited time to seize only those items authorized by the respective search warrants (i.e., the "items to be seized" in Attachment B).[5] The responsive, seizable data was produced in discovery in this case. The government has no legal authority to re-access the Subject Devices (including complete forensic copies thereof) searched pursuant to the warrants that have since expired.

Similarly, for the device for which limited consent was provided by the victim-decedent's next-of-kin (Device No. 1B136), the agents searched the device pursuant to the consent, seized evidence "related to their investigation" (as stated in the consent form), and produced that information to the defense. As reflected in the consent example attached as Exhibit D to defendant's motion, the consent form authorized the FBI (but not the public at large, or defendant) to conduct a "complete search" of the device, permitting only "th[o]se agents" to "take any items, which they determine may be related to their investigation." (Dkt. 28-1, Exh. D, at 48.) The FBI reviewed the device for responsive information, but the consent did not authorize the government to seize all of the data on the device or to turn the entire device over to a third party.

[5] Defendant claims several times that "[n]o search protocols used on the digital devices recovered from the wreckage have been produced in discovery." (Mot. at 3 n.2; see also id. at 9, 9 n.5.) Defendant appears to disregard the extensive search protocols and list of items to be seized found in the Attachment "B"s to the search warrants. (See Dkt. No. 28-1, Exh. C; see also Exh. 1 hereto.) The warrants were produced in discovery; indeed, the defense attaches the *Conception* wreckage search warrant to its motion. (Dkt. No. 28-1, Exh. C.)

The government informed defendant of its position with respect to its lack of authority to re-access the Subject Devices -- much less provide access to other parties -- in September 2022. (See Dkt. No. 28-1, Exh. B, at 7.) The defense has not provided any legal authority in its subsequent correspondence with the government, nor in the instant motion, supporting its position that defendant is entitled to inspect complete copies of the Subject Devices -- and none exists. To the contrary, courts presented with such arguments have consistently reached the commonsense conclusion that defendants cannot compel the government to violate other people's Fourth Amendment rights simply to satisfy a defendant's curiosity.

For example, as the defense is well aware, in United States v. Huizar et al., Judge Walter denied the defendants' motion to compel the government to provide access to full copies of several cooperators' digital devices and email accounts. (See Case No. CR 20-326(A)-JFW.[6]) The Court "reject[ed] the defendants' contention that the Government continues to have authority to either search the devices again for discoverable material or simply turn them over to the defendants." (Exh. 5 at 34:21-24.) The Court concluded that "because the Government is without the requisite legal authority, it is not in the possession of the data for discovery purposes. The Government's possession of the devices and the data that were obtained by search warrant is necessarily circumscribed by the 4th Amendment nor have any of the individuals who own the devices

[6] The government has attached as Exhibit 5 hereto the transcript of the hearing at which Judge Walter ruled on this motion. (See Case No. CR 20-326(A)-JFW, Dkt. No. 597.) The Federal Public Defender's Office, which represents defendant Boylan here, also represents Jose Huizar in the case in front of Judge Walter, and filed the motion to compel in that case. (See No. CR 20-326(A)-JFW, Dkt. No. 381.)

searched pursuant to the warrant consented to a further review of their data." (Id. at 35:25-36:7.)

The Court in Huizar relied in part on United States v. Collins, 409 F. Supp. 3d 228, 244 (S.D.N.Y. 2019), which reached the same conclusion. In Collins, the defendant moved to compel the government to either review devices and accounts belonging to third parties and produce any Brady or Rule 16 material, or to produce the full devices and accounts to the defense. The Court found that the government, having completed its search pursuant to a warrant, "does not have the legal authority to go back and search materials that are non-responsive, i.e., outside the scope of the search warrant." Id. Denying the motion, the Court concluded that the defendants "d[id] not cite any case law to support their proposition that the Government's Brady obligation gives it the legal right to search [a third party's] iCloud data over [the third party's] objection, nor d[id] Defendants explain how such a search would not be inconsistent with [the third party's] Fourth Amendment rights."[7] Id. See also, e.g., United States v. Salyer, 271 F.R.D. 148, 165-66 (E.D. Cal. 2010) (denying defendant's request for access to "a forensic copy of any computer" and access to the email accounts and computers used by cooperating government witnesses, holding that the information was not in the possession of the government and lacked materiality).

Defendant contends that the defense "must be permitted to conduct its own inspection of the devices and should not be limited

[7] As to the limits of consents, the Court observed that "there is no evidence in the record to suggest, that such a consent gives the Government the ability to search the iCloud data in perpetuity without [a third-party's] consent." Collins, 409 F. Supp. 3d at 244 n.17.

to only those items that the government's agent has selected as relevant to the government's case," as to "hold otherwise would lead to an absurd result." (Mot. at 1; see also id. at 11 ("the agents cannot make such a relevancy determination on behalf of the defense").) But the only "absurd result" here would be eviscerating the requirements of Rule 41 and the core tenets of the Fourth Amendment by giving defendants free reign over the entirety of any third party's digital device simply to check the government's work.[8]

The defense's assertion that the FBI agent "selected [items] as relevant to the government's case" misconstrues how Rule 41 search warrants are executed. Every day, federal agents obtain court authorization to search specific property (including digital devices) and then seize only items and information that fall within the scope of Attachment B. Defendants have no role in this search or review process. To the extent the defense seeks to imply the FBI did anything other than seize information responsive to the four corners of Attachment B here, the defense provides no basis whatsoever to question the presumed regularity with which the FBI executes warrants, including those in this case. Nor is the defense's mere desire to have its own look at the victim-decedents' devices contemplated by Rule 41, nor even feasible given the government's lack of access to the Subject Devices. Salyer, 271 F.R.D. at 156 ("[S]imply because the United States obtained documentary information as a result of subpoena or search warrant does not place all documents of those entities or persons within the possession of the

[8] Defendant's erroneous reasoning would similarly eviscerate the requirements and third-party protections of electronic communications search warrants authorized under 18 U.S.C. § 2703.

government for defendant's further requests. The need for formal process in the acquisition of documents is the antithesis of 'access' as defined by the above cases.").

The defense's analogy to the government seizing a file cabinet and seeking to "introduce one document from the cabinet at trial without giving the defense access to the filing cabinet" similarly highlights the defense's distortion of how warrants are executed. (Mot. at 1.) If the government searched a home or office and seized the entirety of a file cabinet as responsive to the warrant, the government would produce the entirety of the file cabinet in discovery. But if the government seized only a portion of the files in the cabinet as responsive to the warrant, the government would not be permitted to re-search the home or office, without new court-ordered authorization, and neither the government nor the defense would have access to the non-responsive files that remained in the cabinet following the search. The same reasoning holds for digital devices, and the defense cites no authority holding otherwise.

Thus, defendant's motion to compel should be denied for the independent reason that the government no longer has possession, custody, or control of the Subject Devices.

2. The Victims' Constitutional and Privacy Rights Further Shield from Disclosure Complete Copies of the Subject Devices

As in virtually all cases involving digital devices, the government was required to obtain court-authorized search warrants or limited consents here to search the victim-decedents' Subject Devices given the Fourth Amendment and the fundamental privacy interests at stake. Those Constitutional constraints and privacy interests are no less paramount now. The Court should preclude the defense from

embarking on a fishing expedition into the victims' most private and personal information that was not identified as responsive to categories of information relating to the fatal *Conception* trip. Such information likely includes communications with their spouses, intimate partners, children, and friends; private photographs and videos; financial information; health information; and innumerable other personal and private matters.

The Supreme Court has recognized that, due to the "immense storage capacity" of cell phones, and their "collect[ion] in one place [of] many distinct types of information -- an address, a note, a prescription, a bank statement, a video" -- the "sum of an individual's private life can be reconstructed" through the data on their personal digital device. Riley v. California, 573 U.S. 373, 393-94 (2014); see also Riley, 573 U.S. at 395-97 (noting that modern smart phone storage capacity "translates to millions of pages of text, thousands of pictures, or hundreds of videos," exposing one to "far more [information] than the most exhaustive search of a house"). In denying the Federal Public Defender's motion to compel in Huizar, Judge Walter similarly recognized that, "the entirety of the [third-party] phone and e-mail accounts" would "contain private, personal, and highly sensitive data," as "the entirety of people's lives in this day and age are typically reflected on their phones, their messages, and e-mails."[9] (Exh. 5 at 37:5-9.)

[9] Notably, the devices and accounts at issue in Huizar belonged to cooperating defendants, categorically distinct from the victim-decedents in this case who could have no cooperation agreements with the government nor any other expectation that their digital devices would ever be disclosed for any purpose.

Notwithstanding the unique status of digital devices under the Fourth Amendment analysis, the defense makes the astounding claim, without citation to any authority, that "[d]igital devices are no different" than the examination of other tangible objects under Rule 16. (Mot. at 6.) But the Supreme Court has found just the opposite, explaining that "[m]odern cell phones, as a category, implicate privacy concerns far beyond those implicated by the search of a cigarette pack, a wallet, or a purse." Riley, 573 U.S. at 393. The defense also contends that courts "routinely permit defendants to forensically examine tangible objects under Rule 16," citing one inapposite out-of-circuit district court case from 1989 (well before the era of ubiquitous smart phones) involving the testing of a sample of cocaine.[10] (Mot. at 6 (citing United States v. Noel, 708 F. Supp. 177, 178 (W.D. Tenn. 1989)).) And the defense seeks to analogize the copying of a "government prepared binder," or the production of "just one side of a double-sided document," to the forensic examination of a modern personal digital device. (Mot. at 1, 6 (citing United States v. Jeffers, 570 F.3d 557, 571-572 (4th Cir. 2009)); id. at 1 (citing United States v. Lee, 573 F.3d 155, 160-61 (3d Cir. 2009)).) The irrelevance of the examples upon which the defense relies for its

[10] Defendant also summarily cites a section of Wright & Miller Federal Practice and Procedure regarding "Discovery by the Defendant – Documents and Tangible Objects" in support of his assertion that courts routinely permit defendants to forensically examine tangible objects. (Mot. at 6 (citing Wright & Miller, 2 Fed. Prac. & Proc. Crim. § 254 (4th ed. 2022)). But remarkably, only one case cited in that treatise -- United States v. Halgat, an inapposite case discussed further herein -- relates to forensic examination of a device, and no other cases cited in the treatise pertain to cell phones, the search of third-party digital devices, or anything remotely similar to the issues here.

central claim regarding forensic analysis of third-party digital devices underscores how unfounded its position is here.

The only case the defense cites having any potential relevance to the digital device context, United States v. Halgat, No. 2:13-cr-241-APG-VCF, 2014 WL 1612686 (D. Nev. Apr. 22, 2014), is distinguishable. (Mot. at 2, 10, 11.) In Halgat, a federal magistrate judge ordered the government to produce an undercover ATF agent's cell phone where the defendant "demonstrate[ed] that the cell phone contain[ed] deleted text messages between Government agents" where they discussed the defendant and the subject drug trafficking operation. Id. at *5-6. Thus, the digital device there belonged to a federal agent (i.e., the government), not a third party -- and much less an innocent victim. The federal agent also had used that digital device in connection with the charges against the defendant. The privacy interests underlying the Fourth Amendment and the government's limitations on accessing third-party devices thus were non-existent in Halgat.[11]

The defense puzzlingly claims that "the purpose of Rule 41 is to protect against illegal searches and seizures by *the government*, and does not bind the conduct of the defense team." (Mot. at 11 (emphasis in original).) But the defense is demanding devices and materials originally seized by the government pursuant to federal court orders, which unquestionably implicates the Fourth Amendment.

---

[11] The defense fails to mention that the government appealed the magistrate judge's order in Halgat, leading to the reversal of orders of production with respect to other government-controlled digital devices. United States v. Halgat, Case No. 2:13-cr-241-APG-VCF, 2016 WL 4528961, at *2 (D. Nev. Aug. 30, 2016) (reversing orders that government produce confidential informant's cell phone and other agents' cell phones where no indication the phones contained information relating to the subject investigation).

What the defense asks the Court to do here, in effect, is order the government to violate the limits of Rule 41, under which it initially received authorization to search the Subject Devices.

The defense ignores the fundamental privacy interests that Rule 41 seeks to protect in its focus on the prophylactic mechanism of the exclusionary rule, which assumes a Fourth Amendment violation has already occurred. (Mot. at 11 (citing United States v. Calandra, 414 U.S. 338, 347 (1974)).) In reliance on Calandra, defendant omits, by an ellipsis, the key point of why it is critical to prospectively protect third-party interests under the Fourth Amendment: "[T]he ruptured privacy of the victims' homes and effects cannot be restored. Reparation comes too late." Calandra, 414 U.S. at 347 (quoting Linkletter v. Walker, 381 U.S. 618, 637 (1965)). There has been no Fourth Amendment violation in this case by the government, and the government's prior search of the Subject Devices did not somehow divest the relevant victim-decedents of their Fourth Amendment and privacy rights.

The same privacy interests still apply to the next-of-kin of the victim who provided a limited consent to the government to search their deceased family member's digital device. Consent must be "unequivocal and specific." United States v. Basher, 629 F.3d 1161, 1167 (9th Cir. 2011) (citation omitted). The standard for measuring the scope of a consent under the Fourth Amendment is that of "objective reasonableness" -- what the typical reasonable person would have understood by the exchange between the individual and law enforcement. Florida v. Jimeno, 500 U.S. 248, 251 (1991). Consent to the FBI to search a loved one's digital device for evidence regarding the circumstances of her death aboard the *Conception* does

not logically support that the consent would extend to the defense team accessing the entire contents of the digital device, beyond the information the government has identified as responsive.

The defense's other arguments seeking to sidestep the Constitution are similarly unavailing. The defense broadly claims, once again without citing any legal authority, that "[p]rivacy interests of third parties are outweighed by a defendant's Constitutional rights to a fair trial, due process, and access to exculpatory information." (Mot. at 10.) The government is not aware of any authority supporting such a vast, blanket proposition, especially with respect to the privacy interests inherent in victims' personal digital devices. The defense offers the analogy of subpoenas issued for "Personal or Confidential Information About a Victim" under Federal Rule of Criminal Procedure 17(c)(3). But Rule 17(c)(3) subpoenas directed, by rule, at third parties (not the government) require "notice to the victim so that the victim can move to quash or modify the subpoena or otherwise object." Rule 17(c)(3) thus recognizes the privacy interests at stake in victim information that defendant seeks to ignore here. See Fed. R. Crim. P. 17, adv. comm. notes on 2008 amendment (explaining requirement for judicial approval for victim information "implements the Crime Victims' Rights Act, codified at 18 U.S.C. § 3771(a)(8), which states that victims have a right to respect for their 'dignity and privacy'").

The defense also asserts that "defendants are allowed to inspect devices containing child pornography to prepare for a criminal trial." (Mot. at 10.) Once again, the defense cites no context or authority for this proposition, but the analogy it seeks to draw is similarly inapposite. The subject devices in child exploitation

cases, by and large, belong to the defendant charged with trafficking in the contraband at issue. A defendant's review in a controlled environment of his own devices in such cases does not implicate the third-party privacy interests at issue here. Nor would a protective order, as the defense suggests (Mot. at 10), alter the fundamental point that the government no longer has possession of the Subject Devices, which have already been searched for responsive data. A protective order also would not remedy the irreparable harm caused by handing over the vast sums of sensitive and non-responsive information likely found on the victim-decedents' Subject Devices. Riley, 573 U.S. at 393-94; Calandra, 414 U.S. at 347.

Thus, regardless of materiality and the government's lack of legal access to the Subject Devices, the motion should be denied because compelling their production would violate the privacy interests and Fourth Amendment protections of the victims.[12]

B. Defendant Has Failed to Make a Threshold Showing of Materiality Under Rule 16

Even if the Court were to find that the full copies of the Subject Devices were within the government's possession, custody, and

[12] While not raised in the motion, the defense has previously argued that the U.S. Attorney's Office supposedly has a "practice" of producing the complete contents of decedents' digital devices in drug overdose cases. (See, e.g., Dkt. No. 28-1, Exh. A (3/5/23 Letter from Defense to Government) at 2.) There is no such "practice," and the fact that individual prosecutors may have voluntarily made such a disclosure in a very small number of cases does not mean that they were required to do so. More importantly, the circumstances in those cases is virtually the opposite of those here: a victim who overdoses may have used his or her phone to communicate with other drug dealers, often in coded language, regarding the acquisition of the drugs that led to their overdose, rendering the victim's communications with third parties potentially relevant. Here, in contrast, the victim-decedents' private communications have no possible relevance to defendant's crime.

control, and the disclosure thereof would not infringe Constitutionally protected privacy interests, defendant's request would fail for a separate reason: the defense has failed to make a threshold showing of materiality. Materiality "requires a presentation of facts which would tend to show that the Government is in possession of information helpful to the defense." Santiago, 46 F.3d at 894-95 (affirming denial of Rule 16 motion where defendant failed to show "case-specific facts which would demonstrate the materiality of the information sought"). "Neither a general description of the information sought nor conclusory allegations of materiality suffice." United States v. Mandel, 914 F.2d 1215, 1219 (9th Cir. 1990).[13]

The defense purports to advance several theories of materiality, all of which are non-specific, conclusory, and without merit.

First, the defense summarily contends that "materiality is established because the government has identified files from the devices it seeks to introduce in its case-in-chief." (Mot. at 7.) This argument defies logic and common sense. That the government identified responsive information on the Subject Devices, which data have been produced to the defense, has no bearing on the data the government found not to be responsive or seizable under the search warrants.

The case upon which the defense relies for this proposition, United States v. Wolfson, 294 F. Supp. 267, 277 (D. Del. 1968), stands only for the unremarkable proposition that materials seized or

[13] Rule 16 is "broader than Brady" because "[i]nformation that is not exculpatory or impeaching may still be relevant to developing a possible defense." United States v. Muniz-Jaquez, 718 F.3d 1180, 1183 (9th Cir. 2013).

obtained that "are necessary to prove the Government's case at trial . . . are obviously material to the preparation of the defense." Id. (case involving "records of corporations with which defendants were connected"). The data that the government did not seize from the Subject Devices are not necessary to prove its case, and thus do not qualify as material on this basis.

Second, regarding the defense's in camera filing purportedly describing a "further explanation of materiality," (Mot. at 7), the government obviously cannot respond. But the motion appears to take issue with the government's scoping of responsive information in the Subject Devices as data "falling within the date range of the diving trip." (Mot. at 9.) Putting aside whether this contention as to scope is accurate, it is difficult to conceive of how any personal information on the deceased victims' devices from before they embarked on the fatal *Conception* trip could have any possible bearing on defendant's criminal misconduct aboard the *Conception*. Whatever theory the defense espouses in camera necessarily would be rooted in conjecture and speculation, which does not suffice for establishing materiality. Mandel, 914 F.2d at 1219.

Third, the defense contends it must be permitted access to the full Subject Devices to accomplish a broad list of non-specific ends, including to "analyze the seized item properly for defense strategy purposes" and to "determine how an artifact was utilized by the user." (Mot. at 8.) These are not "case-specific facts" required to "demonstrate the materiality of the information sought." Santiago, 46 F.3d at 895. Nor are the other non-specific grounds apparently aimed at assessing the authenticity of the seized data and questioning the credibility of the government's sponsoring witnesses

for the data. (See, e.g., Mot. at 8 ("authenticate/validate the files the government produced," "verify the findings of government witnesses about electronically stored information," "verify or dispute the veracity of claims by witnesses pertaining to the digital evidence").)

The defense claims, to that same end, that it needs access to the full devices to "impeach the reliability of computer evidence," including "the government's repairs to the devices and the Cellebrite program used to forensically examine the devices" and "metadata of the files." (Mot. at 7.) To the extent defendant does not stipulate to the authenticity and admissibility of the seized data on the Subject Devices, the government will lay the foundation at trial through witnesses involved in, as necessary, the repairs, extraction, and review of the seized data, which data have already been produced along with other reports regarding the extraction of the data. Moreover, the complete Cellebrite reports and accompanying data produced in discovery provide the defense with the information it would need to seek to challenge the technical aspects of the digital device searches. Access to the non-responsive and non-seized personal information on the Subject Devices, however, could serve no purpose other than to facilitate a fishing expedition or scavenge for impeachment material, which does not suffice for establishing materiality. See, e.g., United States v. Liquid Sugars, 158 F.R.D. 466, 472 (E.D. Cal. 1994) ("[R]equests which are designed to generally cast for impeachment material . . . are not material. Such requests are simply speculative inquiries without basis in fact to

believe that the information acquired will be significantly helpful.").[14]

In any event, with respect to the data seized from the Subject Devices already produced in discovery, unique photos and videos of victims aboard the *Conception* should not present questions of authenticity. Defendant's desire to check the government's work "to determine whether the government's examination was done accurately and completely" (Mot. at 9) is not a substitute for making the required threshold showing of materiality. Santiago, 46 F.3d at 895; Mandel, 914 F.2d at 1219.

For all of the foregoing reasons, the Court should also reject defendant's invitation to compel production of the Subject Devices pursuant to the Court's inherent power to order broader discovery than Rule 16 prescribes. (Mot. at 9.)

C. The Government Also Has Met Its Obligations Under Brady/Giglio

As previously noted, defendant's motion is squarely focused on seeking to compel production of the Subject Devices under Rule 16. Nonetheless, the government also has met its obligations with respect to the Subject Devices under Brady and Giglio.

---

[14] The defense cites two cases from the 1970s in support of its purported need for the full images of the Subject Devices to assess authenticity and credibility. (Mot. at 7-8.) Putting aside that those cases involved computer technology divorced from the privacy implications of modern-day personal cell phones, the cases are further distinguishable in that the computer data the defendants sought to assess were controlled by the government or generated at its behest in the first instance and did not belong to third parties. See United States v. Liebert, 519 F.2d 542, 547 (3d Cir. 1975) ("A major 'witness' confronting Liebert will be computer printouts indicating that the IRS has no record of having received his [tax] returns."); United States v. Dioguardi, 428 F.2d 1033, 1037 (2d Cir. 1970) (government witness "had instructed a computer to prepare figures showing the dates" of certain inventory).

As defendant has failed to meet the requisite threshold showing of materiality under Rule 16, as explained above, he similarly has failed to articulate any credible reason to question the government's satisfaction of Brady, which contemplates a narrower materiality standard than Rule 16 and one that is analyzed retrospectively. See Muniz-Jaquez, 718 F.3d at 1183; see also Bagley, 473 U.S. at 682 ("[E]vidence is material only if there is a reasonable probability that, had the evidence been disclosed to the defense, the result of the proceeding would have been different."). Moreover, the government, not the defense, makes the prospective determination of materiality under Brady. Lucas, 841 F.3d at 807 ("Brady does not permit a defendant to sift through information held by the government to determine materiality.") There is no reason to believe the government has not met its obligation here. See, e.g., Collins, 409 F. Supp. 3d at 244 ("Defendants have not articulated a sufficient reason to believe that the Government's efforts were deficient such that it has failed to meet its Brady obligations.")

Additionally, as with the Rule 16 analysis, the government no longer has access to the Subject Devices to further search them for Brady/Giglio information. Brady's "possession" element "is treated as coextensive with that of Rule 16." United States v. Cano, 934 F.3d 1002, 1023 n.16 (9th Cir. 2019) (citing United States v. Bryan, 868 F.2d 1032, 1037 (9th Cir. 1989); and United States v. W.R. Grace, 401 F. Supp. 2d 1069, 1076 (D. Mont. 2005) ("Whether exculpatory information is in the government's possession for Brady purposes is measured by the same . . . test used under Rule 16(a)(1)(E) for discovery.")). In any event, the government was aware of and

fulfilled its obligations under Brady and Giglio when it had access to, and searched and seized information from, the Subject Devices.

V. CONCLUSION

For the foregoing reasons, the government respectfully requests that this Court deny defendant's motion to compel.